

Harbour Supported Living Services Ltd

170 Seabank Road

Wallasey

Wirral

CH45 1HG

TRANSFERRING PERSONAL DATA POLICY & PROCEDURE

**Transferring Personal Data Policy & Procedure**

**Introduction**

This Transferring Personal Data Policy & Procedure is the overarching policy for data security and protection for Harbour Supported Living Services Ltd (hereafter referred to as "us", "we", or "our").

**Transferring Personal Data**

If an organisation wishes to transfer data to a third party, there are a number of factors to consider, particularly where the transfer is made to an organisation located outside the EU.

**Why is data transferred?**

One of the main reasons that an organisation transfers personal data to another third party is where it needs that third party to do something with the data on its behalf. For example, some organisations outsource their payroll or HR function. Others transfer personal data to pensions and insurance providers, and some to hosted data centres to store the personal data they process. In these scenarios, the recipient of the data becomes the organisation’s data processor.

GDPR requires the organisation (as data controller) and the data processor to enter into a contract containing specific provisions, which are set out in Article 28 of GDPR. The purpose of those provisions is to make sure appropriate obligations are placed on the data processor. Article 28 also requires the contract to specify certain information about the processing that is being carried out, such as the duration and nature of the processing, the purpose of the processing, the types of personal data and the categories of data subjects. This should avoid any confusion between the parties as to what the data processor will do with the data.

You may have already received a number of requests from customers, clients and suppliers asking you to agree to new data protection terms, and this is why!

**Can you transfer data outside of the EEA?**

Yes, but you need to ensure there are appropriate safeguards in place. GDPR ensures that personal data is properly protected if it is transferred throughout the EEA (subject to ensuring there are appropriate agreements in place, as explained above).

Once the personal data leaves the EEA, it’s important to make sure it is still adequately protected. Personal data should only be transferred outside the EEA:

Where the transfer is made to a company located in the USA and the company is Privacy-Shield certified. Privacy Shield replaces the previous “Safe Harbor” scheme and guarantees an appropriate level of protection for personal data transferred to that company. A list of companies that are part of the Privacy Shield scheme can be found here. If the company is not Privacy-Shield certified, alternative safeguards as set out below should be applied; or

Where there has been a finding of adequacy made in respect of the receiving country by the European Commission, guaranteeing that the country provides an adequate level of protection without the need for further safeguards. An up to date list of the countries in respect of which a finding of adequacy has been made can be found here; or Where Privacy Shield doesn’t apply and there is no finding of adequacy, that the transfer is subject to other appropriate safeguards. One of the most frequently used methods of ensuring appropriate safeguards is by incorporating a set of standard contractual clauses that have been approved by the European Commission into the processor agreement. These are known as the “EU Model Clauses". The clauses are in the process of being updated to align with GDPR. The current EU Model Clauses may need to be supplemented with the Article 28 requirements where there is a processor relationship; or

Where the transfer is made between group companies, those companies may implement an intragroup transfer agreement (incorporating the EU Model Clauses) or may introduce binding corporate rules (“BCRs”). BCRs contain provisions governing the transfer and put appropriate safeguards in place. BCRs should be approved by the Information Commissioner's Office and the current waiting time for approval is 12 months.